IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NEBRASKA

UNITED STATES OF AMERICA, Plaintiff, v. MARK RINGLAND, Defendant.	)))))))))	CASE NO. 8:17CR289 **SUPPLEMENTAL BRIEF IN SUPPORT OF DEFENDANT'S MOTIONS [47] & [49]**

Mark Ringland had a reasonable expectation of privacy in his gmail accounts. The warrantless review those accounts and their contents by Google, the National Center for Missing and Exploited Children, and law enforcement over a six-month period infringed upon Mr. Ringland's reasonable expectation of privacy. Furthermore, the warrantless opening and examination of private correspondence by the government and its agents constituted a trespass to chattels in violation of the Fourth Amendment. The contents of these email searches and their fruits should be suppressed.

Having submitted exhibits in support of his motions to suppress and his application for a *Franks v. Delaware*, 438 U.S. 154 (1978) hearing, Dkt. Entries #47 and 49, respectively, Mark Ringland now submits this supplemental brief in support of those motions and asks that those motions and their accompanying briefs be incorporated be reference. This brief merely supplements, and does not replace, those pleadings.

FACTS[1]

I. NCMEC

The National Center for Missing and Exploited Children ("NCMEC") is a non-profit corporation incorporated under the laws of the District of Columbia.[2] It was created to help find missing children, reduce child sexual exploitation, and prevent child victimization.[3]

Two federal statutes, 18 U.S.C. § 2258A and 34 U.S.C. § 11293 (formerly 42 U.S.C. § 5773), mandate NCMEC's collaboration with federal, state, and local law enforcement in the fulfillment of its mission.[4] With partial funding from a Department of Justice grant, NCMEC is required to operate the official national clearinghouse for information about missing and exploited children, to help law enforcement locate and recover missing and exploited children, and to "provide technical assistance and training to law enforcement agencies, State and local governments, elements of the criminal justice system, public and private nonprofit

---

[1] Defendant Mark Ringland asks the Court to find these facts.

[2] Defense Exhibit (D.E.) 144, February 10, 2017 Declaration of John Shehan, Vice President of the Exploited Children Division of NCMEC, *United States v. Miller*, Case No. 2:16CR47 (E.D. Ky.).

[3] *Id.*

[4] *United States v. Ackerman*, 831 F.3d 1292, 1296 (10th Cir. 2016).

agencies, and individuals in the prevention, investigation, prosecution, and treatment of cases involving missing and exploited children."[5]

NCMEC's statutorily-mandated duties include operating a CyberTipLine to provide online users and electronic service providers ("ESPs") such as Google an effective means of reporting Internet-related child sexual exploitation.[6] NCMEC is the first entity to which ESPs must report suspected images of child pornography.[7] NCMEC is, in turn, exempt from provisions that prohibit persons or entities from receiving child pornography.[8]

NCMEC must forward CyberTips to the appropriate federal, state, local, or foreign law-enforcement agency.[9] NCMEC is prohibited from disclosing the information received via the CyberTipLine to any entity other than law enforcement.[10]

Because of the CyberTipLine, Congress has deemed NCMEC a "key component" in the government's efforts to prevent or address offenses committed

---

[5] 34 U.S.C.A. § 11293.

[6] 34 U.S.C.A. § 11293(b)(1)(P).

[7] 18 U.S.C. § 2258A(a)(1); *Ackerman*, 831 F.3d at 1296.

[8] *Ackerman*, 831 F.3d at 1297.

[9] 18 U.S.C. § 2258A(c).

[10] 18 U.S.C. § 2258A(g)(3).

against vulnerable children.[11] According to Congress, NCMEC "works in partnership with the Department of Justice, the Federal Bureau of Investigation, the United States Marshals Service, the Department of the Treasury, the Department of State, the Bureau of Immigration and Customs Enforcement, the United States Secret Service, the United States Postal Inspection Service, and many other agencies in the effort to find missing children and prevent child victimization.[12]

As a reflection of this partnership, members of law enforcement serve on NCMEC's Board of Directors.[13] In 2016, almost a quarter of NCMEC's board was comprised of persons representing government agencies or law enforcement.[14]

Representatives of multiple law-enforcement agencies also have an on-site presence in NCMEC's offices. The representatives include agents from the FBI, Immigration and Customs Enforcement, United States Postal Inspection Service, United States Marshal's Service, and United States Secret Service.[15] The representatives from the FBI include a "supervisory special agent" placed in

---

[11] 34 U.S.C.A. § 11291(10).

[12] *Id.*

[13] D.E. 147, NCMEC 2010 Annual Report, at 20; *see also United States v. Keith*, 980 F.Supp.2d 33, 41 (D. Mass. Nov. 5, 2013); D.E. 144a, September 12, 2012 Testimony of NCMEC ECD Executive Director John Shehan in *Keith*, at 39-41; and *Ackerman*, 831 F.3d at 1298 & n. 5.

[14] *Ackerman,* 831 F.3d at n. 5 (*citing* Board of Directors, NCMEC, http://www.missingkids.com/boardofdirectors)

[15] D.E. 144a, *supra,* at 41; *see also Ackerman*, 831 F.3d at n. 4.

NCMEC's offices to "coordinate the use of both FBI and NCMEC resources and facilitate the most effective response to. . . child pornography, and other cases."[16] The FBI also assigns an intelligence analyst to NCMEC to address cyber tips and support the Child Victim Identification Program.[17] The FBI collaborates with NCMEC to train law-enforcement officers on the CyberTipLine program.[18]

II. GOOGLE

Pursuant to 18 U.S.C. § 2258A(a), Google – as an ESP – must report to NCMEC any apparent violation of the child-pornography laws that Google discovers while providing electronic communication services. Failure to file a report of potential violations results in a substantial fine.[19]

The preferred contents of Google's report to NCMEC are dictated by 18 U.S.C. § 2258A(b), which encourages ESPs to make complete disclosure of information about the individual involved in the communication and the images at issue. Once Google sends a tip to NCMEC, it has a duty under 18 U.S.C, § 2258A(h) to preserve the file on which the report is based.

---

[16] *Ackerman*, 831 F.3d at n. 4.

[17] *Id.*

[18] TR. at 19-20.

[19] 18 U.S.C. § 2258A(e).

To comply with these obligations, Google uses its own proprietary hashing technology which facilitates a comparison of "hash values."[20] A hash value is a short string of characters generated from a larger string of data using an algorithm.[21] The hash value of an image is calculated in a way that makes it unlikely another set of data will produce the same value.[22] Google's hashing technology allows it to search an image's hash value against hash values which have already been assigned to images of child pornography.[23] Some of the previously-flagged images have been identified by Google employees in response to alerts by users of its internet service.[24] Any image with a hash value that matches a hash value in Google's database of contraband images is subjected to further investigation.[25] Upon receiving the alert, or upon encountering a suspect image through other Google business, a trained Google employee might view the image to verify its illegality.[26] If the image depicts child pornography, it is added to Google's repository of illegal images.

---

[20] D.E. 154, Declaration of Cathy A. McGoff, Senior Manager, Law Enforcement and Information Security at Goggle, Inc., in *United States v. Miller*, 2:16CR47 (E.D. Ky.) ("McGoff Declaration"), at 1.

[21] *Ackerman*, 831 F.3d at 1294.

[22] *Id.*

[23] D.E. 154, McGoff Declaration, at ¶ 4.

[24] *Id.* at ¶¶ 4-6.

[25] *Id.* at ¶ 4.

[26] *Id.* at ¶ 7.

In addition to its own hashes, Google benefits from the NCMEC-hosted hash-sharing program.[27] Through this program, NCMEC allows participants to access the hash values of images that other internet service providers have submitted to the CyberTipLine and that NCMEC has verified as child pornography.[28] Google's access to NCMEC's shared database allows Google to broaden its search for contraband images.

Google and NCMEC have described themselves as "partners" in advancing NCMEC's policy of searching out child pornography.[29] As part of that partnership, Google has provided money and technology design to NCMEC.[30] NCMEC has recognized Google as vital to its efforts in curbing the distribution of child pornography.[31]

---

[27] D.E. 154, McGoff Declaration, at ¶ 9; *see also* Government Exhibit (G.E.) 1, July 18, 2018 Declaration of John Shehan, Vice President of ECD, NCMEC, at ¶¶ 21-24.

[28] D.E. 154, McGoff Declaration, at ¶ 9.

[29] *See* D.E. 155, Google Official Blog Entry of June 15, 2013, at 2.

[30] *Id.*; *see also* PR Newswire, "Google Technology Makes Reporting Child Sexual Exploitation Easier" (Dec. 28, 2011), avail. at https://www.prnewswire.com/news-releases/google-technology-makes-reporting-child-sexual-exploitation-easier-136318218.html.

[31] D.E. 157, Washington Post, The Switch: "How Google and Other Tech Firms Fight Child Exploitation," May 6, 2015, at 1.

III. CYBERTIPS

Between March 20, 2017 and September 25, 2017, Google's hashing program combed the contents of two gmail accounts: mringland69@gmail.com and markringland65@gmail.com. The files discovered by Google include some that were sent from one account to itself and some that were not sent at all. Over this six-month span, Google uploaded, in some cases reviewed, and forwarded the contents of these files to NCMEC. Using both automated and manually-entered information, NCMEC reviewed some of the files, investigated the tips, and ultimately converted Google's CyberTips into 35 CyberTipLine Reports, which were then disseminated to law enforcement along with the uploaded files.[32]

Each report is divided into five sections.[33] The first section is the Executive Summary. This section, written by an analyst with NCMEC's Exploited Child Division (ECD), describes the total number of uploaded files sent by Google. It also contains NCMEC's categorization of the material contained in those files, *e.g.*, "Apparent Child Pornography" or "Uncategorized."

Section A follows the Executive Summary. Section A contains "information received in the original submission" from Google, including the URLs (uniform resource locators) of the uploaded files. Deputy Mark Dishaw testified that files with a URL starting with http://lhe.googleusercontent.com and files that had been

---

[32] D.E. 101-108; 112-121; & 128-143.

[33] Not counting the Table of Contents.

uploaded to Google + Photos were most likely found by Google in its Cloud Platform and therefore not accessible to anyone but those having access to the gmail account and Google.[34] Section A also contains information about the user or person being reported and any telephone number, email address, and IP address Google was able to associate with the files. If the user uploaded one of the files to another platform, Section A notes the program to which the file had been uploaded.

Section A also records information provided by Google for each of the uploaded files, asking, "Did Reporting ESP view entire contents of uploaded file?" and "Were the contents of uploaded file publicly available?" Deputy Dishaw testified that for these questions, three answers were possible: yes, no, and Information not provided by company.[35]

Section B reflects NCMEC's automated processing of data provided by Google. For example, if Google sent an IP address to NCMEC with the uploaded data, NCMEC reports in Section B its attempts to geographically link that IP address to a particular location.

Section C details NCMEC's efforts to investigate the CyberTips, identify the reported person or user, and link the report to other CyberTipLine Reports based upon similarities in usernames, phone numbers, and other identifying factors.[36] In

---

[34] TR. at 29-30, 34.

[35] TR. at 31-33.

[36] TR. at 48.

Section C, a NCMEC ECD analyst (whose initials are placed in the Notes section along with a universal time code stamp[37]) manually adds a lettered Priority Level and a classification (*e.g.*, "Apparent Child Pornography") and indicates whether NCMEC has escalated the investigation.[38] If the NCMEC analyst reviewed the uploaded files listed in the CyberTipLine Report, that is mentioned in Section C.[39]

Finally, Section D reports the law-enforcement agencies to which NCMEC disseminated the CyberTipLine Report, the date and time the report was disseminated, and a point of contact for that agency.[40]

In September 2012, then-Executive Director of NCMEC's Exploited Child Division (ECD) John Shehan testified in *United States v. Keith*, 1:11CR10294 (D. Mass.)[41] Mr. Shehan testified specifically about the operation of the CyberTipLine and NCMEC's Hash Sharing Initiative.[42] He explained how ESPs upload content in a CyberTip, which is then assigned to an ECD analyst.[43] The first step for an ECD

---

[37] D.E. 144a at 27.

[38] TR. at 36.

[39] *See, e.g.*, D.E. 111, CyberTipline Report # 21681475, at 4 and D.E. 112, CyberTipline Report #22346425, at 4; *Cf.* D.E. 101, CyberTipline Report #19083866, at 257; D.E. 118, CyberTipLine Report #23002151, at 56; and D.E. 134, CyberTipLine Report #23390937, at 9.)

[40] TR. at 19.

[41] *See* D.E. 144a.

[42] *Id.* at 6, 10.

[43] *Id.* at 10.

analyst, Mr. Shehan noted, "[i]s reviewing the uploaded files[.]"[44] Describing the importance of getting ESPs to upload the content itself to the CyberTipLine, Mr. Shehan testified:

> There have been companies in the past that did not want to upload files into the CyberTipLine. And we have spoken with law enforcement, and they've expressed to us how crucial it is to have those files and information to make that determination. So if there is a company that does not want to upload files, we've suggested that they give a description of what it is they're dealing with, what they've seen.[45]

Once the ESP uploads the file, the URL for the file is deleted and NCMEC maintains the entire record.[46] Mr. Shehan further testified that "law enforcement has access into the CyberTipLine through a virtual private network. They have the ability to come in and download the report. So they would have [the CyberTipLine Report] plus the uploaded file."[47] Asked about how long NCMEC analysts spend on reports, Mr. Shehan answered that it depends, noting that, "[i]f a company doesn't upload 500 files, well, it saves time, you don't have to review as many files."[48]

---

[44] *Id.* at 28; *see also id.* at 48.

[45] *Id.* at 15.

[46] *Id.*

[47] *Id.* at 18; *see also id.* at 30 ("Federal law enforcement have full access to the entire CyberTipLine system.").

[48] *Id.* at 26.

Mr. Shehan also explained that even files that determined by NCMEC analysts to be "not child pornography" (and the accompanying CyberTipLine Report) are provided to federal law enforcement.[49]

In February 2017, Mr. Shehan, now the Vice President of the ECD, submitted a written declaration in *United States v. Miller*, 2:16CR47 (E.D. Ky.)[50] In it, he declared:

> NCMEC is not required to open reported image files or review any content provided by...an ESP in a CyberTipline Report. If NCMEC independently decides to open a reported image file or review the contents of a CyberTipline report, it does so pursuant to its internal organizational and operational guidelines and in furtherance of its private mission to aid children.[51]

Describing NCMEC's February 2017 file-review protocol, Mr. Shehan swore, "NCMEC staff make an independent determination whether to open reported image files based on operational factors, including but not limited to the volume of reports, whether a child might be in imminent danger, and the need to determine a potential geographic location of a child victim or reported user."[52]

Five weeks after Mr. Shehan signed the *Miller* declaration, NCMEC received its first CyberTip from Google regarding mringland69@gmail.com.

---

[49] *Id.* at 50.

[50] D.E. 144.

[51] *Id.* at 3.

[52] *Id.*

IV. MARK RINGLAND

On March 20, 2017, Google scanned and targeted a Gmail account, "mringland69@gmail.com," uploading 784 files from that account and forwarding them to NCMEC.[53] Before doing so, an employee of Google reviewed the contents of some of, but not all of, the 784 files.[54] Specifically, Google reported to NCMEC that it had reviewed the contents of 230 of the 784 uploaded files,[55] but did not specify whether it had reviewed the other 554 uploaded files.[56] With all 784 uploaded files having a "googleusercontent" URL and many of them in Google + Photos, none of the uploaded files in this CyberTip were publicly available.[57] Only four of the 784 files were classified as "apparent child pornography."[58] The remaining 780 were "uncategorized."[59]

---

[53] D.E. 101, CyberTipLine Report #19083866, at 1, 31.

[54] *Id*. at 34-253.

[55] *See id.* (*e.g.*, 5735581ebefea.jpg, thumb_10881.jpg, nelli010.jpg, 026.jpg, ULTRA-MODEL-0846.jpg, thumb_01697.jpg, abby-069.jpg, hmzNtc.jpg, and 180x240_cc30f1dca239f2ef5207.jpg)

[56] *See id.* (*e.g.,* kaYIwQ.jpg, pretty-katia_314.jpg, thumb_10307.jpg, BOJdz0m.gif, thumb_08292.jpg, GLvNp1i.jpg)

[57] *See* TR. at 30, 34.

[58] D.E. 101 at Executive Summary.

[59] *Id.*

The following day, March 21, 2017, Google uploaded and sent to NCMEC 400 more files from mringland69@gmail.com.[60] Google expressly reported it had reviewed the contents of 258 uploaded files. Google did not report whether it had reviewed the remaining 142 uploaded files.[61] None of the 400 uploaded files were publicly available or categorized as "apparent child pornography."

Between April 4, 2017 and April 12, 2017, Google uploaded 30 more files from mringland69@gmail.com to the CyberTipLine, across five CyberTips.[62] Google only reported reviewing the contents of 13 of the 30 uploaded files. None of the uploaded files were publicly available. All 30 files were uncategorized.

On April 17, 2017, having received the seven CyberTipLine Reports and 1214 uploaded files, a NCMEC ECD analyst, LMH, reviewed them.[63] The ECD analyst noted that these reports contain "over 700 files" and "appear to depict

---

[60] D.E. 102, CyberTipLine Report #19153972, at 1, 16.

[61] *Id.*

[62] D.E. 103, CyberTipLine Report #19938982, at 1-2; D.E. 104, CyberTipLine Report #19986242, at 1-2; D.E. 105, CyberTipLine Report #20035870, at 1-2; D.E. 106, CyberTipLine Report #20260729, at 2; and D.E. 107, CyberTip #20293287, at 1. [Note: Each CyberTipLine Report contains two distinct date/time stamps: the date/time Google sent the tip (found in Section A at Incident Information) and the date/time NCMEC received the tip (found on the first page of each report, just above the Executive Summary.)]

[63] *See* D.E. 101 at 257; D.E. 102 at 135; D.E. 103 at 6; D.E. 104 at 7; D.E. 105 at 6; D.E. 106 at 5; and D.E. 107 at 6 (cross-referencing each report with each other and showing an April 17, 2017 processing date.)

new/homemade content."[64] Records checks were conducted on the username, phone number, and one of the IP addresses.[65] One such search of a related telephone number yielded information about a convicted felon, E.G.R.[66] In Section C of CyberTipLine Report #19083866 (D.E. 101), the ECD analyst typed, "I reviewed the uploaded files and found what appears to be CHILD PORNOGRAPHY."[67] The ECD analyst then saved a "Comprehensive Report" and pushed the seven CyberTipLine Reports on to the Nebraska State Patrol.[68]

On April 18, 2017, Google, still combing through the mringland69@gmail.com account, uploaded two more files to the CyberTipLine.[69] Google did not review the contents of either of the uploaded files.[70] Neither of the files were publicly available; neither were categorized as apparent child pornography.[71] On April 28, 2017, the

---

[64] *Id.* Each report notes this.

[65] D.E. 101 at 257-58.

[66] *Id.* at 258-61.

[67] *Id.* at 257 (emphasis in original).

[68] *Id.* at 261, 262; *see also*: D.E. 102 at 136; D.E. 103 at 7; D.E. 104 at 8; D.E. 105 at 7; D.E. 106 at 6; and D.E. 107 at 7.

[69] D.E. 108, CyberTip #20437297, at 1-2.

[70] *Id.* at 2.

[71] *Id.*

same NCMEC ECD analyst, LMH, evaluated this eighth CyberTipLine Report and linked it to the first seven.[72]

By this point, NCMEC had received 1216 uploaded files from Google, of which Google had reported reviewing 501.[73] Of these first eight CyberTipline Reports containing 1216 uploaded files, only four (0.33%) files were categorized as "apparent child pornography." The remaining 1212 (99.67%) uploaded by Google were "uncategorized." None were publicly available.

Armed with these eight CyberTipLine Reports and the contents of the uploaded files, on June 27, 2017, Investigator C.J. Alberico of the Nebraska State Patrol, applied for and received a Douglas County search warrant for the contents of mringland69@gmail.com.[74] In her search-warrant application, Inv. Alberico noted that Google had reviewed 502 of 1216 files and that she had not reviewed any files that Google had not reviewed.[75] Pursuant to the warrant, on July 14, 2017,

---

[72] *Id.* at 4.

[73] For the life of me, 501 is my count. In Investigator Alberico's search-warrant affidavits (D.E. 109, D.E. 122, D.E. 124, and D.E. 126), she says Google reviewed 502. My numbers are: D.E. 101 (230 of 784 reviewed); D.E. 102 (258 of 400 reviewed); D.E. 103 (2 of 6 reviewed); D.E. 104 (3 of 10 reviewed); D.E. 105 (1 of 3 reviewed); D.E. 106 (4 of 4 reviewed); D.E. 107 (3 of 7 reviewed); and D.E. 108 (0 of 2 reviewed). In any event, it's 501 or 502.

[74] D.E. 109, 110.

[75] D.E. 109 at 7.

Investigator Alberico received a thumb drive from Google containing the contents of mringland69@gmail.com.[76]

Meanwhile, Google, seemingly of its own volition and thinking it had found an email account linked to mringland69@gmail.com, scanned Gmail account markringland65@gmail.com on June 19, 2017, uploading two files from it to the CyberTipLine.[77] Before uploading these files, Google did not review their contents.[78] Neither was publicly available.[79] Neither was categorized as apparent child pornography.[80] In the "User or Person Being Reported" section, Google placed "Mark Ringland" under name and noted a secondary email of mringland69@gmail.com. The name "Mark Ringland" does not appear in the "User or Person Being Reported" sections of the first eight CyberTipLine Reports.[81] How Google connected mringland69@gmail.com, markringland65@gmail.com, and the name "Mark Ringland" is unknown.[82]

---

[76] *See* D.E. 124 at ¶ 13.

[77] D.E. 111, CyberTipLine Report #21681475, at 1.

[78] D.E. 111 at 2.

[79] *Id.*

[80] *Id.* at Executive Summary.

[81] *See* D.E. 101-108.

[82] *See* D.E. 124 at ¶ 17, in which case agent Inv. C. J. Alberico avers that "Google provided the name Mark Ringland, associated with the two email addresses mringland69@gmail.com and mringland65@gmail.com."

On June 21, 2017, an ECD analyst, KMT, reviewed this new tip.[83] Here, the analyst noted that s/he had not reviewed the uploaded files.[84] Based upon the use of a South Dakota IP address, NCMEC then pushed the report out to the South Dakota Bureau of Investigation.[85]

On July 12, 2017, Google sent NCMEC two more non-public, uncategorized, and unreviewed files from markringland65@gmail.com, reporting the User or Person Being Reported as "Mark Ringland" with a secondary email address of mringland69@gmail.com.[86]

On July 18, 2017, two NCMEC ECD analysts, KMT and FCM, reviewed CyberTipLine Report #21681475 (D.E. 111) – which had already been reviewed once by KMTon June 21, 2017 – and #22346425 (D.E. 112), respectively. Analyst KMT linked #21681475 to earlier CyberTipLine Reports (*see* D.E. 101-108) and pushed #21681475 to the Nebraska State Patrol.[87] KMT also linked that report to CyberTipLine Report #22346425.[88] Likewise, FCM, reviewing CyberTipLine Report #22346425, linked that report to #21681475 and the first eight reports and pushed it

---

[83] *Id.* at 4.

[84] *Id.*

[85] *Id.* at 6.

[86] D.E. 112, CyberTipLine Report #22346425, at 1-2.

[87] D.E. 111 at 4.

[88] *Id.*

to the Nebraska State Patrol.[89] Just as KMT had done in #21681475, FCM noted that, "NCMEC staff have not opened or viewed any uploaded files submitted with this report and have no information concerning the content of the uploaded files other than the information provided in the report by the ESP."[90]

On July 19, 2017, Google uploaded five more files from markringland65@gmail.com and forwarded them to NCMEC.[91] Google had not reviewed the contents of any of the uploaded files.[92] Google listed "Mark Ringland" as the reported user and included both email addresses.[93] None of five uploaded files listed in this CyberTip were publicly available.[94] Two days later, on July 21, 2017, an ECD analyst reviewed the tip, noting that NCMEC had not reviewed the uploaded files.[95] Nonetheless, NCMEC linked the report to the ten previous reports (D.E. 101-108; 111-112) and forwarded the report and the uploaded files to the Nebraska State Patrol.[96]

---

[89] D.E. 112 at 4-6.

[90] *Id.* at 4.

[91] D.E. 128, CyberTipLine Report #22591470, at 1.

[92] *Id.* at 2.

[93] *Id.* at 2.

[94] *Id.* at 1-2.

[95] *Id.* at Executive Summary.

[96] *Id.* at 4-6.

As of July 21, 2017, Google had uploaded nine uncategorized files from an account in which no apparent child pornography had ever been found. In turn, without reviewing them, NCMEC forwarded those files on to law enforcement.

Between July 31 and August 4, 2017, Google uploaded 1109 more files from markringland65@gmail.com across nine CyberTipLine Reports.[97] None of the 1109 uploaded files were publicly available.[98] Of these 1109 uploaded files, 24 (2%) were categorized as "apparent child pornography;" 1085 (98%) were "uncategorized."[99] Before submitting these reports to NCMEC, Google reviewed 774 of the 1109 files.[100]

An ECD analyst reviewed these nine CyberTips on August 4, 2017.[101] The analyst, FCM – who had, weeks earlier, noted in CyberTipLine Report #22346425

---

[97] *See,* D.E. 113 -121. (Note: D.E. 121, CyberTip #23043630, was submitted by Google to NCMEC on August 4, 2018. Though NCMEC didn't process the tip and forward it to the Nebraska State Patrol until September 5, 2017 – *see* D.E. 121 at 5, 9 – NCMEC did cross-reference the tip in its August 4, 2018 analysis. *See* D.E. 118 at 56.)

[98] As with every uploaded file at issue in this case, Google did not indicate in its CyberTipLine submission that the files were publicly available and every URL of every file demonstrates that the file was drawn from Google's Cloud Platform and, as such, accessible only by Google and the gmail user.

[99] *See* Executive Summaries, D.E. 113-120.

[100] D.E. 113 (21 of 150 reviewed); D.E. 114 (32 of 150 reviewed); D.E. 115 (15 of 93 reviewed); D.E. 116 (147 of 150 reviewed); D.E. 117 (all 150 reviewed); D.E. 118 (147 of 150 reviewed); D.E. (all 33 reviewed) and D.E. 120 (149 of 150 reviewed.)

[101] D.E. 118, CyberTipLine Report #23002151, at 56. (Note: All eight of CyberTipLine Reports refer to CyberTipLine Report #23002151 for analysis. *See* D.E. 113 at 55; DE. 114 at 56; D.E. 115 at 35; D.E. 116 at 58; D.E. 117 at 56; D.E. 119 at 16; D.E. 120 at 55.)

(D.E. 112) that s/he had *not* viewed those files -- typed, "I viewed the uploaded files and found what appears to be APPARENT CHILD PORNOGRAPHY."[102] Eight of the nine reports were sent to the Nebraska State Patrol on August 4, 2017.[103]

On August 7, 2017, Investigator Alberico sought and received a second search warrant from Douglas County (NE) Court.[104] Whereas the first warrant requested the contents of mringland69@gmail.com, the second search warrant requested the contents of two other Gmail accounts: mringland65@gmail.com and markringland65@gmail.com. In this second application, Investigator Alberico – having reviewed the return of the first warrant – averred mringland69@gmail.com had sent images of child erotica and child pornography to mringland65@gmail.com.[105] Investigator Alberico requested the warrant for markringland65@gmail.com on the strength of the newest CyberTipLine Reports.[106] Specifically, Investigator Alberico asserted, "Provided with the nine (9) total CyberTip reports, were one thousand, one hundred nine (1,109) files that contained alleged contraband."[107] On August 18, 2017, Investigator Alberico received from

---

[102] D.E. 118 at 56 (emphasis in original).

[103] D.E. 113-120.

[104] D.E. 122, 123.

[105] D.E. 122.

[106] D.E. 122 at 8.

[107] *Id.*

Google the return of the second warrant, namely the contents of markringland65@gmail.com and mringland65@gmail.com.[108]

Based upon the CyberTipLine Reports and the contents of search-warrant returns, on August 31, 2017, Investigator Alberico sought and received a federal ping warrant for an associated Sprint phone number.[109] The ping warrant placed the target phone at an address on Taylor Street in Omaha. Investigator Alberico thereafter signed a sworn complaint and received federal search and arrest warrants on September 1, 2017.[110]

Meanwhile, though none of this information went into the four search-warrant applications, between August 4 and August 31, 2017, Google uploaded 566 more files from markringland65@gmail.com to NCMEC.[111] Like the thousands before them, none of these files were publicly available. Of these 566 files, Google reported to NCMEC that it had reviewed all but one of them.[112] Six files were characterized as "apparent child pornography." The other 560 files were

---

[108] D.E. 124 at ¶ 25.

[109] D.E. 124, 125.

[110] D.E. 126, 127; Dkt. Entry # 1, 8:17CR289.

[111] *See, generally,* D.E. 129-143. Google sent 97 files in CyberTip #23068622 on August 4, 2017 (D.E. 129 at 1), 41 files in CyberTip #23205331 on August 9, 2017 (D.E. 130 at 1), 150 files in CyberTip #23245909 on August 10, 2017 (D.E. 131 at 1), 36 files in CyberTip #23249764 on August 10, 2017 (D.E. 132 at 1), and 48 files in CyberTip #23274418 on August 11, 2017 (D.E. 133 at 1).

[112] *See* D.E. 131 at 35 (showing "Information Not Provided by Company" for whether Google reviewed file "13 (2).jpg.")

"uncategorized." NCMEC reviewed these uploaded files on August 14, 2017,[113] August 25, 2017,[114] and September 5, 2017,[115] respectively, linking them to older CyberTipLine Reports, and forwarded them to the Nebraska State Patrol. The August 25, 2017 ECD reviewer, CLH, stated affirmatively, "I reviewed the uploaded files and found content which appears to be CHILD PORNOGRAPHY."[116]

On September 1, 2017, law enforcement executed the federal search and arrest warrants at the Taylor Street address.[117] Mark Ringland was arrested, cell phone in hand. He was taken to a police car, *Mirandized*, and questioned.[118] During the questioning, he made incriminating statements and authorized law enforcement to retrieve an electronic device from his van, parked nearby.

---

[113] *See* D.E. 131 at 54-56 (cross-referencing the CyberTipLine Reports found at D.E. 129-133) and referring the reader to D.E. 118 (CyberTipLine Report #23002151) "for all analysis"; *see also* D.E. 129 at 28, D.E. 130 at 18, D.E. 132 at 16, and D.E. 133 at 20, referring the reader to D.E. 131, CyberTipLine Report #23245909, "for all analysis.")

[114] *See* D.E. 134 at 9 (cross-referencing the CyberTipLine Reports found at D.E. 134-139) and referring the reader to D.E. 118 (CyberTipLine Report #23002151) "for all analysis"; *see also* D.E. 135 at 10, D.E. 136 at 18, D.E. 137 at 18, D.E. 138 at 17, and D.E. 139 at 4, referring the reader to D.E. 134, CyberTipLine Report #23390937, "for all analysis.")

[115] *See* D.E. 140 at 5 (cross-referencing the CyberTipLine Reports found at D.E. 140-143); *see also* D.E. 141 at 7, D.E. 142 at 4, and D.E. 143 at 11, referring the reader to D.E. 140, CyberTipLine Report #23625155, "for all analysis.")

[116] D.E. 134 at 9.

[117] D.E. 163 at 4.

[118] D.E. 163 at 4.

On September 5, 2017, Investigator Alberico transported Mr. Ringland from the Douglas County (NE) Correctional Center to the federal courthouse in Omaha.[119] During the ride, Mr. Ringland made further statements about the allegations against him.[120]

LAW

The Fourth Amendment protects "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures...."[121] A "search" triggers the Fourth Amendment when the government infringes upon an expectation of privacy that society considers reasonable.[122] A search can also trigger the Fourth Amendment "when it involves a physical intrusion (a trespass) on a constitutionally protected space or thing ("persons, houses, papers, and effects") for the purpose of obtaining information."[123]

An email is a paper or effect for the purposes of the Fourth Amendment.[124]

---

[119] D.E. 163 at 4-5.

[120] *Id.*

[121] U.S. Const., amend. IV.

[122] *See United States v. Jacobsen*, 466 U.S. 109, 115 (1984).

[123] *Ackerman*, 831 F.3d at 1307 (*citing United States v. Jones*, 565 U.S. 400, 407-08 (2012) (emphasis in original)).

[124] *See, e.g., United States v. Ackerman*, 831 F3d 1292, 1304 (10th Cir. 2016) ("No one in this appeal [including the United States or amici curiae, NCMEC and Google, Inc.] disputes that an email is a 'paper' or 'effect' for Fourth Amendment purposes.")

Emails – particularly unsent emails – and files saved in email accounts are private. Society is prepared to recognize a reasonable expectation of privacy in individual email accounts. In *Riley v. California*, 134 S. Ct. 2473 (2014), the Supreme Court, holding that the government needs a warrant before it can search the content of an individual's cell phone, commented upon contemporary society's view of the digital privacy:

> Modern cell phones, as a category, implicate privacy concerns far beyond those implicated by the search of a cigarette pack, a wallet, or a purse. A conclusion that inspecting the contents of an arrestee's pockets works no substantial additional intrusion on privacy beyond the arrest itself may make sense as applied to physical items, but any extension of that reasoning to digital data has to rest on its own bottom.
>
> Cell phones differ in both a quantitative and a qualitative sense from other objects that might be kept on an arrestee's person. The term "cell phone" is itself misleading shorthand; many of these devices are in fact minicomputers that also happen to have the capacity to be used as a telephone. They could just as easily be called cameras, video players, rolodexes, calendars, tape recorders, libraries, diaries, albums, televisions, maps, or newspapers.[125]

Just as cell phones have, in the 21st century, become repositories for calendars, maps, and diaries, email accounts have become our 21st century post offices and file cabinets. These accounts are private. Google accounts are password-protected and use two-factor authentication.[126] Individual users frequently use a variation of their

---

[125] 134 S. Ct. at 2489.

[126] *See,* Brian X. Chen & Nicole Perlroth, "How Google's Physical Keys Will Protect Your Password," NY Times, Oct. 25, 2017 (available at https://www.nytimes.com/2017/10/25/technology/personaltech/google-keys-advanced-protection-program.html) ("Google was one of the first companies to start offering

name or nickname. The warrantless opening and examination of private correspondence that could have contained much besides contraband "seems pretty clearly to qualify as exactly the type of trespass to chattels that the framers sought to prevent when they adopted the Fourth Amendment."[127]

The mere use of a corporate email server, like Gmail, does not relinquish one's privacy interest. Recently, in *Carpenter v. United States*, 138 S.Ct. 2206 (2018), the Supreme Court declined to extend the third-party doctrine of *Smith v. Maryland*, 442 U.S. 735 (1979), and *United States v. Miller*, 425 U.S. 435 (1976), to historical cell-site location information.[128] In *Carpenter,* the Court noted that, "[a] person does not surrender all Fourth Amendment protection by venturing into the public sphere. To the contrary, 'what [one] seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected.'"[129] Critiquing the government's invocation of the third-party doctrine, the *Carpenter* Court acknowledged that it had,

---

two-factor authentication back in 2010, not long after it learned that it had been hacked by state-sponsored Chinese hackers. After the attack, Google's security team came up with a motto, 'Never again.' The company later rolled out two-factor authentication for Google customers' Gmail accounts.")

[127] *Ackerman*, 831 at 1307-08 (*citing, e.g.*, 1 Thomas M. Cooley, The General Principles of Constitutional Law in the United States of America 212 & n. 2 (1880); Thomas M. Cooley, A Treatise on the Constitutional Limitations Which Rest Upon the Legislative Power of the States of the American Union 306 n.2 (1868); and *Ex Parte Jackson*, 96 U.S. 727, 733 (1877)).

[128] 138 S.Ct. at 2223.

[129] *Id.* at 2217 (*quoting Katz v. United States*, 389 U.S. 347, 351-52 (1967)).

in *Smith* and *Miller*, "drawn a line between what a person keeps to himself and what he shares with others."[130] The government's reliance upon the third-party doctrine, the Court held, "fails to contend with the seismic shifts in digital technology that made possible the tracking of not only Carpenter's location but also everyone else's, not for a short period of time but for years and years."[131]

Similar seismic shifts permit Google and other ESPs, which enjoy billions of users, to review, track, and submit to the government thousands of otherwise private files and personal correspondence.

Having established that email accounts are private, we turn to the question at hand: Were Google's and NCMEC's warrantless searches of Mark Ringland's private email accounts Fourth Amendment-implicating events?

Yes, they were.

ANALYSIS

I. Google, a government agent, conducted repeated warrantless Fourth Amendment searches of Mark Ringland's email.

The Fourth Amendment applies only to state action.[132] The only way a private party can conduct a Fourth Amendment search is if it acts as an agent or instrument

---

[130] *Id.* at 2216.

[131] *Id.* at 2219.

[132] *Jacobsen*, 466 U.S. at 113.

of the government.[133] If a statute compels the private party to conduct a search, the private party acts as a government agent.[134] If even a statute or regulation "so strongly encourages a private party to conduct a search that the search is not 'primarily the result of private initiative,'" the private party acts as a government agent under the Fourth Amendment.[135] "[S]ince time out of mind the law has prevented agents from exercising powers their principals do not possess and cannot delegate."[136]

In this case, Google, operating under the authority of and under the coercion of a statutory scheme requiring them to send contraband to the government, uploaded thousands of private files from two Gmail accounts to NCMEC's CyberTipLine. The instant Google uploaded these files, they were available to be opened and reviewed by the government – first by NCMEC, a government entity, and then by law enforcement, who have access to the CyberTip network through a VPN and to whom "every single report, no matter what, is made available."[137]

---

[133] *Id.*

[134] *Skinner v. Ry. Labor Executives' Ass'n*, 489 U.S. 602, 614 (1989).

[135] *United States v. Stevenson,* 727 F.3d 826, 829 (8th Cir. 2013) (*quoting Skinner v. Ry. Labor Executives' Ass'n*, 489 U.S. 602, 614-15 (1989)).

[136] *Ackerman*, 831 F.3d at 1300 (*citing* 1 William Blackstone, Commentaries *417-20 and Restatement (Second) of Agency § 17 (1958))

[137] D.E. 144a at 50.

Between March 20, 2017 and September 25, 2017, Google acted as an agent of the government. Google entered into this agency relationship as a sort of half-volunteer, half-conscript. A federal statutory scheme "so strongly encourages" searches of email that Google's searches are not "primarily the result of private initiative."[138] Section 2258A of Title 18, U.S. Code, imposes a duty upon "whoever, while engaged in providing an electronic communication service or a remote computing service to the public through a facility or means of interstate or foreign commerce" to "provide to the CyberTipline of the National Center for Missing and Exploited Children" a report should the provider obtain actual knowledge of apparent violations of ennuerated federal statutes. "ISPs who fail to comply with this obligation face substantial (and apparently criminal) penalties payable to the federal government."[139]

The Eighth Circuit, reviewing a similar but distinguishable set of facts in *United States v. Stevenson*, 727 F.3d 826, 830 (8th Cir. 2013), held that "[a] reporting requirement standing alone, does not transform an Internet service provider into a government agent whenever it chooses to scan files sent on its network for child pornography." In *Stevenson*, America Online (AOL), using its hash-detection process, discovered that an AOL account belonging to Stevenson had emailed child

---

[138] *Stevenson*, 727 F.3d at 829 (*quoting Skinner*, 489 U.S. at 614-15.)

[139] *Ackerman*, 831 F.3d at 1296 (*citing* 18 U.S.C. § 2258A(a)(1)).

pornography to a Google email account.[140] The *Stevenson* Court acknowledged that (1) an ESP search to assist law enforcement and (2) government knowledge of and acquiescence in a private search are two factors that could prompt a finding of agency.[141] But, the Court held, because Stevenson had failed to provide a reason to believe those factors were present, the district court did not abuse its discretion in denying the motion without a hearing.[142]

Here, however, we have a different story. Urged on by a statutory scheme and with the government aware of and acquiescing in its ongoing searches, Google went above and beyond to assist in the investigation of Mark Ringland.[143]

First, Google – which has offered no position in this case – was actively involved in the investigation of these accounts. Of the first 1216 files that Google uploaded to the CyberTipLine, only four had been categorized as apparent child pornography. Google has provided no basis for sending NCMEC the other 1212 files. Altogether, of the 2898 files that Google uploaded across these 35 CyberTips, Google sent NCMEC 2865 uncategorized, non-public files (98.8 % of the total) from these Gmail accounts.

---

[140] 727 F.3d at 828.

[141] *Id.* at 830 (*citing United States v. Smith,* 383 F.3d, 700, 705 (8th Cir. 2004)).

[142] *Id.* at 830-31.

[143] *See Smith*, 383 F.3d at 705 (8th Cir. 2004); *see also Stevenson*, 727 F.3d at 830.

Google's participation increased considerably as NCMEC and law enforcement got involved. From March to July, Google seemed to passively upload files, reviewing just 40% of the files in the CyberTips. By late July/early August, however, Google ramped up its involvement. Of the 1109 files uploaded between July 31 and August 4, Google employees manually reviewed 70% of them. Of the 566 files uploaded after August 4, Google employees reviewed 99.8% – all but one. And it was Google – not NCMEC or law enforcement – that connected the two email addresses and first named "Mark Ringland" as the user. These protracted, independent investigatory acts suggests that Google remained an active participant in this investigation well beyond the initial CyberTips.

And second, as NCMEC's numerous CyberTipLine Reports and Investigator Alberico's search-warrant affidavits demonstrate, the government was well aware of Google's ongoing searches of Mark Ringland's email accounts. Beginning with the receipt of more than 1200 files in March 2017, NCMEC was on notice that Google was combing mringland69@gmail.com. The Nebraska State Patrol received that information in April. By May 12, 2017, Investigator Alberico had submitted a preservation letter to Google.[144] As the CyberTipLine Reports trickled in – first to NCMEC and then to the State Patrol – those agencies knew that Google had continued the search of mringland69@gmail.com, linked two Gmail accounts,

[144] D.E. 163 at 1.

repeatedly scanned markringland65@gmail.com, and identified "Mark Ringland" as the user of those accounts.

Put simply, the very facts that the *Stevenson* Court declared could prompt a different outcome are present in Mark Ringland's case. While *Stevenson* involved a limited timeframe, the present case shows a back-and-forth between the agencies and Google participating at a degree not seen in *Stevenson.* Considering the facts of *this* case, Google acted as an agent of the government and conducted numerous, warrantless Fourth Amendments searches of Mark Ringland's Gmail accounts. *Nothing* about *Stevenson* demands that Ringland's motions be denied. In fact, it does quite the contrary.

Google's decision to act as a citizen cop is a not insignificant affront to privacy. "Google currently counts at least seven products with more than one billion users: Android, Chrome, Google Play, Gmail, Maps, Search, and YouTube."[145] In February 2016, Google reported that Gmail had more than one billion monthly active users.[146] As of July 2017, that number had climbed to 1.2 billion.[147] In October 2015, Google +

---

[145] D.E. 159, Ken Yeung, "Google Photos passes 500 million users, gets better sharing features and $10 photo books." Venturebeat.com, May 17, 2017, at 1.

[146] D.E. 158, Frederic Lardinois, "Gmail Now Has More Than 1B Monthly Active Users." Techcrunch.com, February 1, 2016, at 1.

[147] Motek Moyen, "Gmail is Very Popular But Google Still Won't Fix a Security Vulnerability." SeekingAlpha.com, July 17, 2017 - https://seekingalpha.com/article/4088241-gmail-popular-google-still-fix-security-vulnerability

Photos had 100 million active users.[148] That number doubled eight months later.[149] As of May 2017, Google+ Photos is an application being used by more than 500 million monthly active users with more than 1.2 billion photos uploaded.[150] Google is like the Sprint Corporation in *Carpenter*: "not your typical witness[]. Unlike the nosy neighbor who keeps an eye on comings and goings, [it is] ever alert, and [its] memory is nearly infallible."[151] Instead of keeping track of your location, however, Google is the postman who opens your mail, forwarding on to law enforcement not just contraband, but anything that remotely resembles it – even "a clearly adult type of image."[152]

II. Even if Google's acts were not Fourth Amendment searches, NCMEC, a government entity, expanded upon Google's searches.

The "calling card of a governmental entity is whether it is 'invested with any portion of political power, partaking in any degree in the administration of civil government, and performing duties which flow from sovereign authority.'"[153] The

---

[148] *Id.*

[149] *Id.*

[150] D.E. 159, *supra*, at 1.

[151] 128 S.Ct. at 2219.

[152] D.E. 144a at 50 (where Mr. Shehan testifies that even images deemed not child pornography are still forwarded to the authorities. "Every single report, no matter what, is made available to federal law enforcement.")

[153] *Ackerman*, 831 F.3d at 1295 (*quoting Trustees of Dartmouth College v. Woodward*, 17 U.S. (4 Wheat.) 518, 668-69, 4 L.Ed. 629 (1819)).

National Center for Missing and Exploited Children enjoys law-enforcement powers beyond those enjoyed by private citizens. Two statutes – 18 U.S.C. § 2258A and 34 U.S.C. § 11293(b) – "mandate its collaboration with federal (as well as state and local) law enforcement in over a dozen different ways, many of which involve duties and powers conferred on and enjoyed by NCMEC but no other private person."[154] "NCMEC and NCMEC alone is statutorily obligated to maintain an electronic tipline for [ESPs] to report possible child sexual exploitation to the government."[155] Moreover, ESPs are required to report contraband to NCMEC, who, in turn, requires the ESP to preserve the evidence.[156]

The Tenth Circuit's opinion in *Ackerman* addresses a fact pattern, present here, not considered by the Eighth Circuit in *Stevenson*: where NCMEC – a government entity – engages in a search that is more expansive than the one conducted by the ESP. Under those facts, the *Ackerman* Court found that a Fourth Amendment search by a government entity had occurred.[157] In this case, NCMEC reviewing hundreds of files that Google did not.

---

[154] *Ackerman*, 831 F.3d at 1296.

[155] *Ackerman*, 831 F.3d at 1296. [Note: The *Ackerman* Court uses "ISP" in lieu of "ESP." The terms are, it would seem, interchangeable.]

[156] *See* 831 F.3d at 1297.

[157] *See* 831 F.3d at 1306.

The government, in its reply [58], has argued that "Ringland's reliance upon *United States v. Ackerman*, 831 F.3d 1292 (10th Cir. 2016) is both factually and legally misplaced."[158] The government goes on to argue, without citation, that "NCMEC changed its rules and procedures in response to the Tenth Circuit's decision in *Ackerman*. NCMEC will not view an image that was not previously viewed by the Electronic Service Provider."[159] And the day before the hearing the United States produced a declaration of John Shehan stating, "In February 2014,[160] NCMEC engineered and implemented a filter for the CyberTipLine to block staff from being able to view an uploaded file unless the ESP indicates it personally reviewed the uploaded file or the uploaded file was publicly available as identified in Section A of the report."[161]

But that doesn't seem to be the case.

On April 17, 2017, an ECD analyst at NCMEC, LMH, reviewed seven CyberTips. These CyberTips reported information on each of 1214 "uploaded files." In the Executive Summary of the primary CyberTipLine Report, the analyst noted, "This is a report that from Google containing uploaded files that appear to depict apparent child pornography. The report contains over 700 uploaded files; some of

---

[158] Dkt. Entry #58 at 2.

[159] *Id.* at 10.

[160] *Ackerman* was decided in August 2016.

[161] G.E. 1 at ¶ 19 (footnote not in original).

the files are unfamiliar to me." The tables of contents painstakingly list an entry for each of 1214 "uploaded files." Within the notes section of Section C of the primary CyberTipLine report, the analyst again noted that the report contained over 700 files, including "uploaded files that appear to depict new/homemade content." Finally, the analyst stated unequivocally, "I reviewed the uploaded files and found what appears to be child pornography." These reports – crafted by an analyst as these tasks are performed – should be taken at face value. They describe without qualification the review of "the uploaded files," of which there were 1214.

The government will reply, "Well, in Section C, the phrase 'uploaded files' refers only to the 500 files Google reviewed." This explanation flatly ignores the Executive Summary where the analyst refers to the "over 700 uploaded files, *some of* [*which*] *are unfamiliar to me*." It also ignores the February 2017 sworn declaration of John Shehan in the *Miller* case in the Eastern District of Kentucky. In that declaration – sworn out just one month before Google began sending CyberTips in this case – Mr. Shehan not only fails to mention this three-year-old filter, but goes on to list the criteria by which ECD analysts decide whether to open files.[162]

Miller, it would seem, would have been the *perfect* case for Mr. Shehan to mention this filter. In *Miller*, Google hadn't reviewed the images in the lone CyberTip.[163] If a filter existed in February 2017 that blocked ECD analysts from

---

[162] D.E. 144 at ¶ 12.

[163] *See* D.E. 154, McGoff Declaration, at ¶ 11.

reviewing files that hadn't been reviewed by the ESP, and if Google hadn't reviewed the files in *Miller*, why doesn't John Shehan's *Miller* declaration just say that the filter prevented NCMEC from opening the files? Instead of providing a list of criteria? The implication is clear: NCMEC had the capacity in 2017 to open files that hadn't been reviewed by the ESP. If it didn't, Mr. Shehan would have said so.

Curiously, in *Miller*, the receiving law-enforcement agency *did* open the attachments and view the images.[164] It seems odd that law enforcement would be able to open an attachment from NCMEC that NCMEC could not open itself.

That implication is, again, bolstered by the *express* statements of NCMEC's analysts that they reviewed the uploaded files. These statements stand in marked contrast to a handful of CyberTipLine Reports where ECD analysts note that they *haven't* reviewed the files. In D.E. 111, D.E. 112, and D.E. 128 – CyberTips where Google reported having viewed *none* of the files – three separate ECD analysts affirmatively stated that NCMEC had not reviewed the files, a fact that should have been self-evident if, at this point, NCMEC had been three years into a curiously self-imposed filtration system. Three weeks later, on August 4, 2017, one of those analysts (FCM), reviewing CyberTips covering 1109 "uploaded files" (of which Google had only viewed 774), affirmatively reported that s/he had "viewed the uploaded

[164] *United States v. Miller*, 2:16CR47, Dkt. Entry #41, Report & Recommendation, at 4.

files."[165] FCM, who has a history of noting when files were not reviewed, did not qualify this statement in any way – *e.g.*, with a "some" or "most."

Indeed, several days later, when Investigator Alberico submitted her application for a search warrant in Douglas County on August 7, 2017, she gives the impression that these 1109 files had been reviewed by NCMEC. Specifically, she reported:

> On August 7, 2017, Your Affiant received information that nine (9) more CyberTip reports had been submitted by Google, Incorporated to NCMEC.... Provided with the nine (9) total CyberTip reports, were one thousand one hundred nine (1,109) files that contained alleged contraband....Not all files were reviewed by Google, Incorporated and Your Affiant has not reviewed these files.[166]

Knowing that Google had only reviewed 774 of the files and knowing that she herself had reviewed none of them, Investigator Alberico's statement that 1109 files (essentially *all* of the files before ECD analyst FCM on August 4, 2017) contained alleged contraband must have come from somewhere. If neither Google nor Investigator Alberico had reviewed these files, process of elimination suggests that it was NCMEC. This deductive reasoning is only bolstered by FCM's unequivocal declaration, "I viewed the uploaded files."

The evidence dictates that on April 17, 2017, an ECD analyst reviewed 1214 uploaded files, of which Google had already reviewed 501 or 502. Based, at least in

---

[165] D.E. 118 at 56.

[166] D.E. 122 at 8.

part, upon a NCMEC analyst's assertion (though attributed to Google in the application) that some of these files contained child pornography and that they contained new/homemade content, a county judge issued a search warrant that yielded the full contents of mringland69@gmail.com. On August 4, 2017, an ECD analyst reviewed 1109 files, of which Google had reviewed 774. Based upon the information included in the first application, information received as a result of the first warrant, and the implication that NCMEC had concluded that these 1109 files "contained alleged contraband," a second warrant was issued that yielded the full contents of two other email addresses. Between March 2017 and September 2017, NCMEC, a government entity, repeatedly expanded upon Google's searches and, as such, conducted warrantless searches of Mr. Ringland's effects. This expansion alone constitutes a warrantless Fourth Amendment search.

The evidence further dictates that John Shehan's July 18, 2018 declaration – particularly ¶ 19 – is not credible. Either the filter did not exist or NCMEC ECD analysts found a way around it.

III. The good-faith exception does not save these warrantless searches.

The government hopes to convince the Court that, because Investigator Alberico obtained search warrants, the good-faith exception should save the dozens of warrantless searches that supported her warrant applications. The law, however, precludes this.

In *United States v. Leon*, 468 U.S. 897, 913 (1984), the Supreme Court held that evidence obtained by officers acting in reasonable reliance on a warrant issued by a detached and neutral magistrate, yet later found to be unconstitutional, is nevertheless admissible. The *Leon* Court held that the good-faith exception, however, does not apply in the following situations: (1) when the warrant is based on an affidavit containing a knowing or reckless falsity, *Franks v. Delaware,* 438 U.S. 154 (1978); (2) when the magistrate has acted simply as a "rubber stamp" for law enforcement officers; (3) when the affidavit is "so lacking in indicia of probable cause as to render official belief in its existence entirely unreasonable," (4) when the warrant is so "facially deficient" in failing to particularize the place to be searched or things to be seized that an officer could not reasonable rely on the warrant; and (5) when the warrant itself was a fruit of a prior illegal search.[167]

The "good-faith" exception does not apply to Ringland's case. Each of the four warrants issued in this case were fruits of the prior illegal searches. Without Google's CyberTips and NCMEC's expansive reviews of the uploaded files, Investigator Alberico's search-warrant affidavits would have been blank below the caption.

CONCLUSION

Google continues to comb through the files and correspondence of its 1.2 billion users, forwarding questionable files onto NCMEC who in turn passes them to

[167] *Leon*, 468 U.S. at 923.

law enforcement. Even if these private files turn out to be legal, their delivery to and review by the government cannot be undone. It is only through cases like Mark Ringland's that the courts, recognizing the rationales undergirding *Riley* and *Carpenter*, can affirm society's reasonable expectation of privacy in its correspondence. Using the agency factors articulated in *Stevenson*, ths Court should find that, in this case, Google acted as an agent of the government. Ths Court should also find that NCMEC, by reviewing thousands of files that Google had not reviewed, expanded upon Google's searches and, in doing so, triggered the Fourth Amendment.

Suppression of the evidence obtained illegally as a result of the warrantless searches by Google, NCMEC, and the Nebraska State Patrol is the proper remedy here. All evidence seized from Mr. Ringland's gmail accounts, his person, his ZTE cell phone, and his iPad, as well as all statements taken from him, should be suppressed as fruit of these illegal searches. *Wong Sun v. United States*, 371 U.S. 471, 487-88 (1963).

MARK RINGLAND, Defendant,

By: s/ Richard H. McWilliams
Richard H. McWilliams 22455
Assistant Federal Public Defender
222 South 15th Street, Ste. 300N
Omaha, NE 68102
(402) 221-7896
rich_mcwilliams@fd.org

CERTIFICATE OF SERVICE

I hereby certify that on August 10, 2018, I filed the foregoing with the Clerk of the Court on CM/ECF which prompted the transmission of an electronic copy to: Michael Norris, Assistant United States Attorney, Omaha, NE.

s/ Richard H. McWilliams